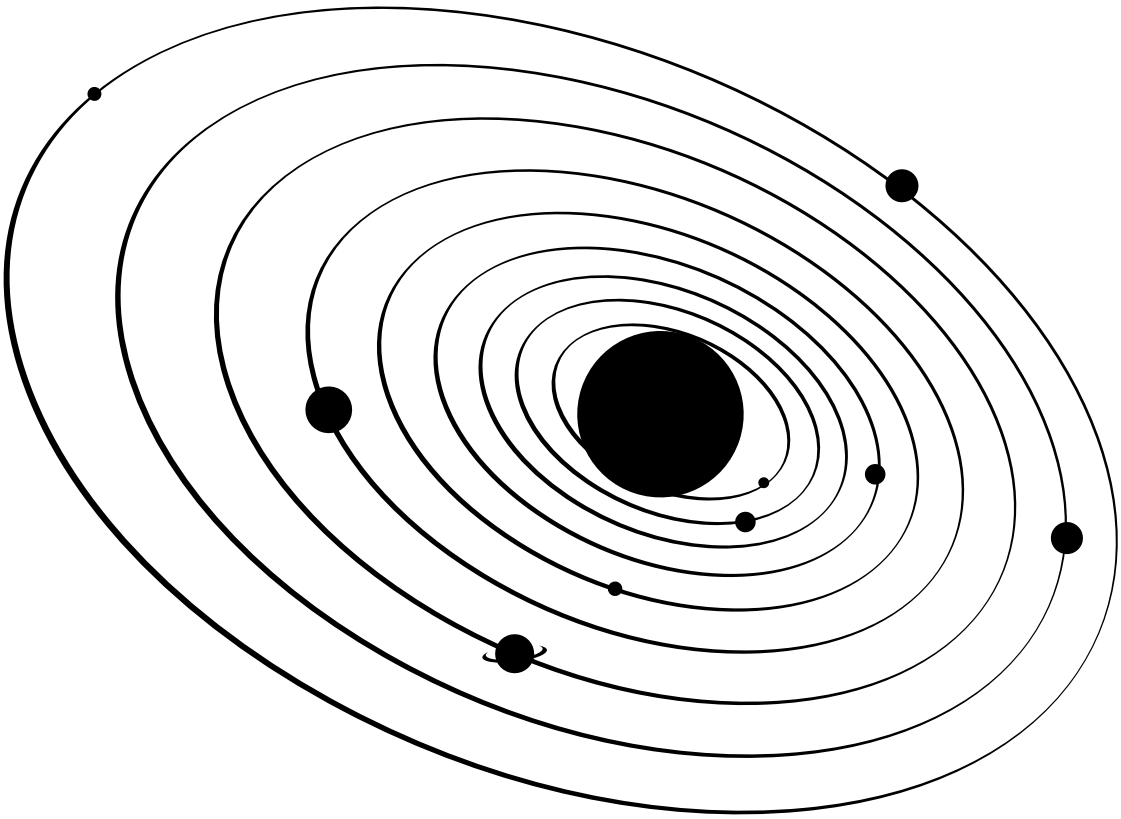
Centre for International
Governance Innovation

CIGI Papers No. 277 — June 2023

Interplanetary Internet Governance

Laura DeNardis



Centre for International
Governance Innovation

CIGI Papers No. 277 — June 2023

Interplanetary Internet Governance

Laura DeNardis

About CIGI

The Centre for International Governance Innovation (CIGI) is an independent, non-partisan think tank whose peer-reviewed research and trusted analysis influence policy makers to innovate. Our global network of multidisciplinary researchers and strategic partnerships provide policy solutions for the digital era with one goal: to improve people's lives everywhere. Headquartered in Waterloo, Canada, CIGI has received support from the Government of Canada, the Government of Ontario and founder Jim Balsillie.

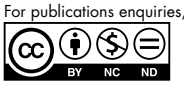
À propos du CIGI

Le Centre pour l'innovation dans la gouvernance internationale (CIGI) est un groupe de réflexion indépendant et non partisan dont les recherches évaluées par des pairs et les analyses fiables incitent les décideurs à innover. Grâce à son réseau mondial de chercheurs pluridisciplinaires et de partenariats stratégiques, le CIGI offre des solutions politiques adaptées à l'ère numérique dans le seul but d'améliorer la vie des gens du monde entier. Le CIGI, dont le siège se trouve à Waterloo, au Canada, bénéficie du soutien du gouvernement du Canada, du gouvernement de l'Ontario et de son fondateur, Jim Balsillie.

Credits

Managing Director and General Counsel Aaron Shull
Director, Program Management Dianna English
Project Manager Jenny Thiel
Publications Editor Susan Bubak
Senior Publications Editor Jennifer Goyder
Graphic Designer Brooklynn Schwartz

For publications enquiries, please contact publications@cigionline.org.



67 Erb Street West
Waterloo, ON, Canada N2L 6C2
www.cigionline.org

Table of Contents

About the Author

Laura DeNardis is a CIGI senior fellow and professor and endowed Chair in Technology, Ethics, and Society at Georgetown University. She is recognized as a leading internet governance expert in both the United States and the world. *Wired UK* named her one of "32 Global Innovators Who are Building a Better Future" and her book *The Internet in Everything: Freedom and Security in a World with No Off Switch* (Yale University Press, 2020) was recognized as a *Financial Times* Top Technology Book of 2020. Among her seven books, *The Global War for Internet Governance* (Yale University Press, 2014) is considered a definitive source for understanding power struggles over the digital world. Laura is an affiliated fellow of Yale Law School's Information Society Project, where she previously served as executive director, and is a member of the Council on Foreign Relations. She holds an A.B. in engineering science from Dartmouth College, a master of engineering from Cornell University, a Ph.D. in science and technology studies from Virginia Tech, and was awarded a post-doctoral fellowship from Yale Law School.

Acronyms and Abbreviations

ARPA	Advanced Research Projects Agency
ARPANET	Advanced Research Projects Agency Network
ASAT	anti-satellite
ASN	autonomous system numbers
BGP	Border Gateway Protocol
CCSDS	Consultative Committee for Space Data Systems
CERT	computer emergency response (or readiness) teams
CIR	critical internet resources
CNSA	China National Space Administration
CSA	Canadian Space Agency
CSIRT	computer security incident response teams
DARPA	Defense Advanced Research Projects Agency
DNS	Domain Name System
ESA	European Space Agency
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
ICTs	information and communication technologies
IETF	Internet Engineering Task Force
IoT	Internet of Things
IP	Internet Protocol
IPR	intellectual property rights
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISO	International Organization for Standardization
ISS	International Space Station
ITU	International Telecommunication Union
IXP	internet exchange point
JAXA	Japan Aerospace Exploration Agency
JPL	Jet Propulsion Laboratory
NASA	National Aeronautics and Space Administration
OEWG	Open-Ended Working Group
OSI	Open Systems Interconnection
OST	Outer Space Treaty
PGP	Pretty Good Privacy
RFC	Request for Comments
RIPE NCC	Réseaux IP Européens Network Coordination Centre
RIRs	regional internet registries
TCP/IP	Transmission Control Protocol/ Internet Protocol
UNGA	United Nations General Assembly
UNOOSA	United Nations Office of Outer Space Affairs

Executive Summary

The internet's next chapter will likely lie in both infinitesimally small and astronomically large spaces, including a leap further off Earth and into deep space. Already, engineers are working on a solar-system internet and developing new protocols to withstand the harsh conditions and colossal distances of space. As the internet moves off planet, so too will internet governance and its attendant economic, political and social implications. The security implications are immense. What are the internet governance arrangements — meaning the technical design, institutional coordination, norms of behaviour and legal instruments — that should be anticipated now to help operationalize an interplanetary internet for the good of humankind? This paper lays out deep-space challenges to internet architecture and governance, examines the relevance of existing UN space governance treaties to digital networks, discusses which layers of terrestrial internet governance could be applicable in space, and suggests some geopolitical lessons from the history of the terrestrial internet that might inform a solar-system internet and its emerging "heliopolitics."

Introduction

The internet might not exist in its contemporary form without space exploration. Against the backdrop of the Cold War, the Soviet Union successfully launched the first artificial Earth satellite, Sputnik, in 1957. The American public and policy makers alike viewed this as a potential crisis for both national security and technological leadership. New institutions and rapid technological innovation followed. Within a year of the Sputnik launch, the United States passed the National Aeronautics and Space Act establishing the National Aeronautics and Space Administration (NASA), and also founded the Advanced Research Projects Agency (ARPA) credited with the early innovations that directly led to the global internet. Indeed, developments in space have shaped the development of the internet on Earth.[1]

Is it too soon to discuss an interplanetary internet, never mind its governance? History suggests no. The modern internet barely existed a half century ago. The Advanced Research Projects Agency Network (ARPANET) dates back only to the late 1960s, around the same time NASA successfully carried out the Apollo 11 lunar landing and Gordon Moore founded microprocessor company Intel in an area of California later called Silicon Valley. The founders of Google and Facebook were not yet born. Even the rise of the World Wide Web only dates back to the early 1990s, when there was no Amazon, smartphones, Internet of Things (IoT) or streaming video. The pace of technological transformation has been stunning as the internet has diffused into every corner of the Earth, around our planet's atmosphere, into material objects and even into the human body.

The internet's next frontier likely lies in both infinitesimally small and astronomically large spaces, with both areas involving cyber-physical interfaces and embedded artificial intelligence. Digital technologies have already diffused into miniscule spaces such as nano-devices and wirelessly connected objects inside the human body, but will also become more expansive as the internet extends into outer space.

Already, engineers are working on a solar-system internet and developing new protocols to withstand the harsh conditions and colossal distances of space. NASA is developing the LunaNet network around the Earth's Moon, and the European Space Agency (ESA) is working on a similar lunar telecommunications project called Moonlight. Humans are embarking on a new age of discovery and exploration in space. The Mars Perseverance rover and other scientific equipment are searching for a history of microbial life and collecting data previously unimaginable. The James Webb Space Telescope is peering at objects as they were 13.6 billion years ago when light left early stars and galaxies. Anyone visiting Florida's Space Coast can see regular SpaceX launches

1 ARPA became the Defense Advanced Research Projects Agency (DARPA), which describes its origin as follows: "The genesis of that mission and of DARPA itself dates to the launch of Sputnik in 1957, and a commitment by the United States that, from that time forward, it would be the initiator and not the victim of strategic technological surprises." See www.darpa.mil/about-us/about-darpa.

with reusable rockets landing back on Earth on autonomous drone ships. Human settlement of space that was once the purview of science fiction is now imaginable because of rapid advancements in everything from robotics, sustainable energy, rocket propulsion and 3D printing, to low-gravity medical and food advancements.

The future of space exploration depends upon the future of a resilient, secure and interoperable deep-space communication system. Extending conventional nomenclature from Earth, this network could be called the "interplanetary internet," a solar-system internet or space network. Internet pioneer Vinton Cerf broached the subject of an "interplanetary internet" at an Internet Society meeting in Geneva, Switzerland, in July 1998 (Kaiser 1998, 879). Online references to the term do not exist prior to this, except in one lone encyclopedia entry on Cerf describing his distinguished visiting scientist appointment "working on the design of an interplanetary Internet" at the Jet Propulsion Laboratory (JPL).[2] Indeed, the inception of work on an interplanetary internet began at NASA's JPL in 1998 (King 2007). This vision was remarkable in a time before most modern internet applications.

In March 1999, not long after the founding of Google, NASA administrator Daniel S. Goldin gave a "Pathway to the Future" presentation at NASA's Langley Research Center, presenting a vision for the future of NASA. This dot-com era vision prominently featured a "space station" and a "Mars plane" as well as "interplanetary Internets" (Goldin 1999).

Reminiscent of the early ARPANET days when only a few universities were connected and no one could have anticipated what the internet would mean to the world, it may not yet be possible to imagine the innovative uses of such a network. What can be anticipated, though, are uses of networks in space to support discovery and exploration; to interconnect space stations; to communicate with environmental sensors, 3D printers and other cyber-physical and autonomous objects; and to support human space travel and a range of conceivable commercial uses as well as the inevitable national security and intelligence applications. Many initiatives in space already use communication networks, such as JPL's Deep Space Network. Most of these are point-to-point communication networks between the Earth and spacecraft. The idea of a solar-system internet is more of a store-and-forward, distributed, packet switched design that interconnects many nodes and multiple networks. Designing and building an interoperable and secure infrastructure is a necessary precursor for anything to happen in space as well as for human security on Earth. National security on Earth is increasingly dependent upon networks in space.

Internet governance is not fixed any more than technology is fixed. "Internet governance" is a broad term meant to capture an entire ecosystem of actors carrying out the coordination and administration of the technologies that keep the internet operational and the enactment of policy around these technologies. In a literal sense, internet governance is an oxymoron because it is not just about traditional governments and legal instruments but also about decisions made by private industry, international organizations and technical coordinating organizations, and by the very design of technical architecture. Some of these tasks include standards setting, oversight of unique names and numbers, interconnection agreements, cybersecurity governance, and the public policy role of private infrastructure and media companies whose decisions shape conditions of privacy, surveillance, speech and digital security. Some functions involve one actor. Many involve coordination across different kinds of actors. Together, this collection of tasks is usually called "multistakeholder internet governance."

What was once the esoteric domain of technical specialists, some academics and specialized governmental agencies has landed at the top of global policy agendas. Politicians at the highest level speak about cyber governance in the same breath as other pressing global problems such as war, terrorism, human rights and the environment. How governance decisions around digital infrastructure unfold has deep consequences for the economy, critical infrastructure protection, the political sphere, consumer safety, speech, innovation policy and national security. The internet is in everything. Internet governance is therefore entangled with most public policy problems.

As the internet moves off planet, so will internet governance and all its economic, political and social implications. The security implications alone are immense. What are the internet governance arrangements — meaning the technical design, institutional coordination and legal instruments — that should be anticipated

2 See https://encyclopedia2.thefreedictionary.com/Vinton+gray+cerf.

now to help operationalize an interplanetary internet for the good of humankind? Is this just an extension of terrestrial internet governance, or do the unique political and material contexts of space require something new? Are existing space treaties relevant? What types of public interest requirements have to be designed now into the architecture? What cooperation among nation-states is necessary to invest in and benefit from this network? Under what agreements and assurances should networks connect?

Because there is not yet an interplanetary internet, examining the coordination points and political tensions around this emerging infrastructure is an exercise in anticipatory governance. Scholars of science and technology studies conceptually embrace "anticipatory governance" with an objective of constructing emerging technologies that consider human flourishing and human security.[3] Anticipatory governance can be defined as "a broad-based capacity extended through society that can act on a variety of inputs to manage emerging knowledge-based technologies while such management is still possible" (Guston 2014, 219).

Technical design itself is an act of anticipatory governance because political objectives and social values as well as practical problem solving, shape and embed within technical architecture.[4] Internet governance has often evolved organically and reactively, such as building in security and authentication systems somewhat after the fact. There is a moment of opportunity to anticipate the technical coordination functions and heliopolitical structures necessary in space to architect a shared interplanetary communication future that benefits all humankind. As such, this paper proceeds in four parts. The first section, "Deep-Space Features Shaping Internet Architecture and Governance," examines the unique constraints of space that will shape interplanetary network architecture and governance. The next section, "Relevance of Existing International Space Treaties to the Internet," assesses the applicability of these treaties and governance frameworks to deep-space information and communication technologies (ICTs). The following section, "A Framework of Multistakeholder Internet Governance in Space," examines the core layers of internet governance on Earth most likely to extend into deep space, which ones do not apply and what might be missing. The final section, "Internet Governance Flashpoints Applicable in Space," concludes the paper by suggesting some geopolitical lessons from terrestrial internet governance that might inform structures of interplanetary internet governance and its emerging heliopolitics.

Deep-Space Features Shaping Internet Architecture and Governance

Unique constraints and contexts in space will shape design and governance in this domain. Some are natural, involving harsh atmospheric conditions, astronomical distances and planetary rotation. Others are human originating, such as the dangerous conditions caused by space debris. Still other features are political, such as the way sovereignty is upended in space. The terrestrial system of internet architecture and governance cannot just be extended into space, but must be reconceptualized and re-engineered to meet these novel conditions.

Space Debris

On November 15, 2021, the Russian Federation destroyed a Soviet-era satellite that had been launched in 1982 (NASA 2022, 1). While the first concern of a direct-ascent anti-satellite (ASAT) missile test may be a national security one around the weaponization of space, a more immediate threat materialized. According to NASA's *Orbital Debris Quarterly News* account of this intentional destruction, the US Space Force used the Space Surveillance Network to identify "more than 1500 pieces of large, trackable fragments" from the breakup (ibid.). Two months later, the China National Space Administration (CNSA) announced that a Chinese satellite experienced a "near miss" with one of the fragments from the Russian ASAT test debris field (Jones 2022).

The Chinese government itself had previously conducted an ASAT test resulting in a massive

3 See, for example, Jasanoff (2016).

4 See, for example, Winner (1980); Latour (1992); Bowker and Starr (1996).

space-debris field. On January 11, 2007, a Chinese ASAT system test hit an "old Chinese meteorological spacecraft, Fengyun-1C," resulting in roughly 2,000 dangerous fragments greater than 5 cm in size and approximately 35,000 fragments greater than 1 cm in size (NASA 2007, 2). The United States and India have also, at various times, conducted direct-ascent ASAT missile tests (NASA 2019, 1). It is not so much the size, but the speed, that poses the danger. Space debris — which hurtles along at rates so fast they are measured in miles per second rather than miles per hour — are already a risk for the International Space Station (ISS), rockets and satellites orbiting the Earth.

As exploration and communication moves off Earth, human-originating space debris — sometimes called "space junk" — will likely join natural debris (such as micrometeorites) as a space-specific source of disruption that must be anticipated and addressed in protocol design; architectural resiliency and fault-tolerant approaches; redundancy, error detection and correction; and policy and industry attention to tracking.

Delay and Disruption

"The speed of light is too slow," Cerf famously said about the delay problem caused by the astronomical distances between objects in space (D'Agostino 2020). The speed of light is 3×10^8 metres per second (or 186,000 miles per second), the reason why light from the sun, roughly 93 million miles from the Earth, takes eight minutes to reach Earth. Humans never see the sun in real time, but rather the way it appeared eight minutes ago. NASA signals between Deep Space Network antennas on Earth and the orbiters around Mars that relay signals from the Perseverance rover take between five and 20 minutes (double that for a round-trip signal). The wide variation primarily relates to the solar-system position of Earth and Mars at the moment of transmission. The issue is not just delay but also variable delay due to the constantly shifting relative distances and locations of solar-system objects.

Because of this constant movement of celestial objects, and also planetary rotation, these objects can rotate out of connectivity. The movement of planets and their satellites will create constantly changing transmission distances and intermittent disruptions. Add this to the potential disruptions from space debris encounters and, especially, the natural disturbances caused by planetary magnetic fields, solar flares and asteroids.

These delay and disruption conditions will upend much of how systems of internet architecture and governance work in space. Many existing network engineering principles are not applicable. The assumption that transmission loss is relatively small collapses. Retransmission as the usual response to error correction or packet loss is not an ideal approach. These conditions will require new design choices that add store-and-forward memory capacity, such as in routers. On Earth, routers do not store packets but rather just forward them. From a technical perspective, systems of internet governance that require multiple transmissions, such as those involving Domain Name System (DNS) lookups, or cybersecurity approaches involving considerable back and forth, will not be ideal in space or even feasible in many cases.

Coordinating systems around authentication, identity, error detection and correction, address translation and compression will have to adjust to massive latency and routinized packet loss. Design principles will require greater autonomy in network nodes, local processing capability on routers, store-and-forward approaches rather than dropping packets, possibly smaller packet sizes, and the elimination of network approaches requiring round-trip session establishment. Indeed, engineering work is already under way. The very charter for the Internet Engineering Task Force's (IETF's) Delay/Disruption Tolerant Networking Working Group, for example, aspires to "data communications in the presence of long delays and/or intermittent connectivity."[5]

The critical implication for internet governance is that the infrastructures of connectivity and coordination now prevalent, from routing and addressing to the DNS, will require fundamental redesigns or replacements.

Node Intelligence and Autonomy

One of the early design principles of the internet was to locate intelligence at end points. This principle is upended in space. More autonomy, memory and self-resiliency will be expected of information and communication nodes in space because of routine broken connectivity and limitations due to long physical distances. Nodes

5 See https://datatracker.ietf.org/wg/dtn/about/.

in deep space will need to function even when networks are disrupted, and require self-sufficient and renewable power, intrinsic memory and microprocessing power flexibly capable of carrying out multiple tasks. Swapping out a damaged or obsolete component will be nearly impossible in real time, so maintenance and upgrades will have to be largely local or controlled remotely.

A solar-system internet will be, in some ways, similar to IoT cyber-physical networks on Earth. To have useful applications for discovery and exploration, networks will embed directly or otherwise interact with the physical world of space. Some devices will embed sensors that gauge temperature, pressure, movement, chemical readings and other physical characteristics. Some will have actuators that "act" on the world through some output such as rotary motion, linear motion, heating, cooling, pressure, and so forth. Deep-space networks will be as much like cyber-physical systems (for discovery and exploration) as the screen-based internet of human communication (for human transmission from space stations, space craft and beyond). In addition to embedding additional intelligence and memory to address delay and disruption, operational nodes may also embed sensors and actuators. But unlike IoT devices, which are often engineered for ad hoc specific purposes and design parsimony, deep-space nodes will be broad-purpose and versatile devices.

All of the constrained architectural requirements facing interplanetary internet nodes — the need for renewable power, local processing power and memory, heterogenous functionality and maintenance self-sufficiency — all come down to one design principle: autonomy.

Time Synchronization in Variable Gravitational Fields

Timekeeping is an underappreciated and taken-for-granted aspect of internet governance, and computer networking in general. So much depends upon time synchronization. Atomic clocks ultimately serve as the source of time standardization on Earth and — by keeping time based on the resonant frequencies of atoms — are far more precise than rotational time keeping such as of the Earth on its axis (days), the Moon around the Earth (months) or the Earth around the sun (years). Coordinated Universal Time is the Earth's atomic-clock-based standard. Among other synchronizing approaches, the Network Time Protocol has long been the standard for helping computing devices keep in time synchronization to universal atomic time.

The new challenge in space is that, according to theories of relativity, time is slower or faster in different gravitational fields. For example, because of the Moon's lower mass than the Earth, its gravitational field is weaker. Therefore, a clock on the Moon would run faster than a clock on the Earth. The time synchronization required for network transmission and coordination is challenged by time relativity and especially how different gravitational conditions affect clock speed.

Sovereignty and Extraterritoriality

Scholars have mulled over complications of nation-state jurisdiction relative to the internet on Earth since the 1990s.[6] Laws and policies apply to technologies and institutions within national borders, but even this is upended because so much of the technical architecture crosses borders in ways that have no natural correspondence to nation-states.[7] The internet's logical (software-defined) architecture is already border-agnostic. A single exchange can involve a domain name registration in one region, cross-border content distribution networks, and transmissions originating and terminating in one country but switched through an internet exchange point (IXP) in another country. This porousness has led countries to assert cyber sovereignty claims and techniques that turn to institutions and infrastructures for political control (Musiani et al. 2016). Overlaying a Westphalian international relations model on terrestrial cyberspace does not comport with either cross-border technologies or the resulting levers of infrastructure control by extraterritoriality.[8] At the same time, what happens locally can have cascading effects, such as local blocking of a website accidentally disseminated to the global internet via Border Gateway Protocol (BGP).[9]

6 See, for example, Wu (1997). See also Johnson and Post (1996).

7 For a broad literature review of cyber sovereignty scholarship, see Mueller (2020).

8 For a detailed theoretical examination of digital sovereignty via infrastructure "situated practices," see Musiani (2022).

9 For one example, see Singel (2008).

In space, there is no sovereignty over celestial bodies and free space, at least not at this time and under current international treaties. But this does not preclude conflicts over cyber sovereignty and territorial disputes in space. It is also possible that the upending of sovereignty could have benefits for a communication system. Regardless, in space, international relations theory and international law could be further upended or possibly more relevant than ever.[10] While there are analogies to cyber sovereignty tensions on Earth and also the Law of the Sea on Earth, the expansive reach and challenges of outer space make this domain *sui generis*.

The pragmatic, theoretical and legal limits to nation-state control or ownership of outer space are, in themselves, inherent political features, but will be further complicated by extensions into space of extraterritorial control exerted in the terrestrial internet via co-opting infrastructure, the privatization of governance and the ways in which local actions cascade outward. Jurisdiction is already disrupted by features of the terrestrial internet. The contemporary nature of sovereignty in space will further complicate internet governance and require greater cooperation and negotiation among multiple stakeholders, as well as new heliocentric political frameworks. Reciprocally, the technologies extended into space will affect the international order on Earth because so much of national security and economic resiliency depends upon space systems.

Relevance of Existing Space Treaties to the Internet

Space is already governed by a constellation of treaties and alliances, many of which arose during the mid-twentieth-century space race between the United States and the Soviet Union.[11] In the Cold War context, very few nations had any programs for space exploration. The Soviet Union launched Sputnik in 1957. The United Nations launched the United Nations Office for Outer Space Affairs (UNOOSA) the following year, in 1958. UNOOSA's Committee on the Peaceful Uses of Outer Space became the forum for international treaties and principles on space-related activities[12] (UNOOSA 2022). Out of this institutional context came five foundational UN space treaties (UNOOSA 2017) (see Table 1). The first one, the Outer Space Treaty (OST), arose contemporaneously with and in the same geopolitical and technological context as ARPANET. The last of the five main treaties was adopted the same year Apple released the original Macintosh computer and prior to the development of the World Wide Web. Since that time, there have also been bilateral and other multilateral agreements, such as the Artemis Accords. To what extent are they applicable to communication networks in deep space?

The cornerstone of space governance is the OST. In 1967, the UN General Assembly (UNGA) adopted this foundational Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies to establish that space exploration and use should be "for the benefit of all" humankind and open to all states, as well as not subject to sovereign appropriation.[13] States also agree to not place nuclear weapons and other weapons of mass destruction in space and to use the Moon and planets only for peaceful purposes. Originally signed by the United States, the United Kingdom and the Soviet Union, more than 100 countries have since become parties to the treaty.

The Rescue Agreement quickly followed in 1968, elaborating on the core principles of the OST. The UN treaty, officially called the Agreement on the Rescue of Astronauts, the Return of Astronauts and the Return of Objects Launched into Outer Space, committed to — exactly as the title indicates — the rendering of assistance to astronauts in distress, the return of astronauts in

10 For an analysis of international relations theory and the space domain, see Pace (2023).

11 For a more detailed history and description of the treaties and laws applicable to space, see Aganaba (2021).

12 All of the UN Space Law Treaties and Principles are available through UNOOSA at www.unoosa.org/oosa/en/ourwork/spacelaw/treaties.html.

13 *Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies*, 27 January 1967, Res 2222 (XXI) (entered into force 10 October 1967), online: <www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/outerspacetreaty.html>.

Table 1: The Five UN Foundational Space Treaties

	Year				
	1967	1968	1972	1976	1984
Treaty name	The Outer Space Treaty	The Rescue Agreement	The Space Liability Convention	The Registration Convention	The Moon Agreement

the event of an emergency landing and the return of space objects.[14] The text from the original Rescue Agreement from the 1960s helps convey the tone and style of the agreement — around international cooperation, peaceful exploration, freedom and mutual aid — very much through the lens of nation-state authority and UN coordination.[15]

In 1972, the Convention on International Liability for Damage Caused by Space Objects (the Space Liability Convention) opened for signature and took force to hold nation-states responsible for any damage caused by a "space object."[16] In 1976, the Convention on Registration of Objects Launched into Outer Space went into force to track the increasing number of so-called space objects placed into orbit or launched for various purposes.[17] The Registration Convention is essentially a tracking agreement requiring registration of objects launched into outer space. The meaning of the word "tracking" is quite different than in the cyber realm and does not mean real-time tracking but just a registration of orbital and functional details. While written in the context of launching states, the registration of objects launched from a nation-state — submitted to UNOOSA for inclusion in the space registry — includes private enterprises. For example, the US submissions to the registry often include dozens or hundreds of private satellite launches, as shown in Table 2.[18] The July 2022 submission alone included more than 200 Starlink satellites. The space object registry, as it has evolved over time, includes submissions from Belgium, Canada, Chile, China, ESA, Finland, France, Germany, Greece, Guatemala, India, Indonesia, Japan, Luxembourg, Malaysia, Mauritius, New Zealand, South Korea, the Republic of Moldova, Slovenia, Spain, the Russian Federation, Tunisia, Turkey, Ukraine, the United Arab Emirates, the United Kingdom and the United States, among others.

The Moon Agreement is different in kind in that the treaty has not been signed by any of the major human spaceflight countries, including China, Japan, the Russian Federation, the United Kingdom or the United States. One of the concerns, among others, involved the treaty's call for establishing an "international regime" for governing natural resources from the Moon, and the imprecision about what that might mean. Yet it entered into force for its ratifying parties in 1984 as the Agreement Governing the Activities of States on the Moon and Other Celestial Bodies to lay out numerous provisions about the Moon, such as prohibiting rights of ownership, calling for lunar resources not being subject to appropriation or international conflict, and essentially calling for a framework of laws establishing international cooperation and a commitment to environmental protection and equality, among other provisions.[19] The agreement prohibits the establishment of

14 *Agreement on the Rescue of Astronauts, the Return of Astronauts and the Return of Objects Launched into Outer Space*, 19 December 1967, Res 2345 (XXII) (entered into force 3 December 1968), online: <www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/rescueagreement.html>.

15 Ibid., Annex, art 2, online: <www.unoosa.org/pdf/gares/ARES_22_2345E.pdf>.

16 *Convention on International Liability for Damage Caused by Space Objects*, 29 March 1972, Res 2777 (XXVI) (entered into force 1 September 1972), online: <www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/liability-convention.html>.

17 *Convention on Registration of Objects Launched into Outer Space*, 14 January 1975, Res 3235 (XXIX) (entered into force 15 September 1976), online: <www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/registration-convention.html>.

18 *Information furnished in conformity with the Convention on Registration of Objects Launched into Outer Space*, Note verbale dated 7 November 2022 from the Permanent Mission of the United States of America to the United Nations (Vienna) addressed to the Secretary-General, 15 November 2022, UN Doc ST/SG/SER.E/1079, online: <www.unoosa.org/oosa/osoindex/data/documents/us/st/stsgser.e1079.html>.

19 *Agreement Governing the Activities of States on the Moon and Other Celestial Bodies*, 18 December 1979, Res 34/68 (not yet entered into force), online: <www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/moon-agreement.html>.

Table 2: US Submissions to the UNOOSA Space Registry, July 2022 (Excerpt)

International Designation	Name of the Space Object	Date of the Launch	Location of the Launch	Basic Orbital Characteristics				General Function of the Space Object	Date of Decay
				Nodal Period (Minutes)	Inclination (Minutes)	Apogee (km)	Perigee (km)		
2022-076BA	Starlink-4151	July 7, 2022	AFETR	91.53	53.22	351	348	C	-
2022-076BB	Starlink-4157	July 7, 2022	AFETR	91.53	53.22	351	348	C	-
2022-076BC	Starlink-4155	July 7, 2022	AFETR	91.53	53.22	351	348	C	-
2022-076BD	Starlink-4153	July 7, 2022	AFETR	91.53	53.22	351	348	C	-
2022-076BE	Starlink-4156	July 7, 2022	AFETR	91.53	53.22	351	348	C	-
2022-077A	Starlink-4362	July 11, 2022	AFWTR	94.57	97.66	499	496	C	-
2022-077B	Starlink-4349	July 11, 2022	AFWTR	94.47	97.66	494	492	C	-
2022-077C	Starlink-4350	July 11, 2022	AFWTR	94.47	97.66	494	492	C	-
2022-077D	Starlink-4331	July 11, 2022	AFWTR	94.47	97.66	494	492	C	-
2022-077E	Starlink-4352	July 11, 2022	AFWTR	94.46	97.66	494	491	C	-
2022-077F	Starlink-4355	July 11, 2022	AFWTR	94.77	97.66	509	506	C	-
2022-077G	Starlink-4345	July 11, 2022	AFWTR	94.75	97.66	508	505	C	-
2022-077H	Starlink-4343	July 11, 2022	AFWTR	94.76	97.66	508	506	C	-
2022-077J	Starlink-4336	July 11, 2022	AFWTR	94.73	97.66	507	504	C	-
2022-077K	Starlink-4341	July 11, 2022	AFWTR	94.75	97.66	508	505	C	-
2022-077L	Starlink-4337	July 11, 2022	AFWTR	94.73	97.66	507	504	C	-
2022-077M	Starlink-4339	July 11, 2022	AFWTR	94.74	97.66	507	505	C	-

Source: www.unoosa.org/oosa/en/spaceobjectregister/index.html.
Note: AFETR = Air Force Eastern Test Range; AFWTR = Air Force Western Test Range; C = spacecraft engaged in practical applications and uses of space technology such as weather or communications.

military bases on the lunar surface and placing into lunar orbit weapons of mass destruction.

Collectively, these existing space governance treaties do not directly address ICTs and are not easily applicable to the cyber domain. This is, in part, because the treaties predate most internet technologies. They neither address routine human communication over networks, nor the emerging vision of space networks connecting cyber-physical systems such as additive manufacturing (for example, 3D printing) and IoT devices.

The treaties also predate mass satellite proliferation and the complete and total national and societal strategic dependency on satellites on Earth. Losing satellite communication on Earth would be catastrophic. Some of the societal functions that depend upon space communications include transportation systems and GPS navigation, financial transactions including time-stamping of financial transactions, weather forecasting, television and entertainment broadcasting, first responder communications and internet access, among many other critical operations on Earth.

They also predate terrestrial national security dependency on space systems, including real-time monitoring, drone navigation, and command-and-control networks. Space is an operational domain for the North Atlantic Treaty Organization. There is now a rebranded French Air and Space Force and a US Space Force armed service, established in 2019 by the National Defense Authorization Act with the motto "*semper supra*" ("always above") and a mission to both "protect U.S. and allied interests in space and to provide space capabilities to the joint force."[20] Space is considered a domain of warfare that is just as strategic as other domains.

The overall space governance framework is quite different from internet governance frameworks, one largely multilateral and one largely multistakeholder. Internet governance is not based on treaties and international law and has historically been multistakeholder, a very contested term and model of governance but one that realistically captures the role of private actors in the design, administration and governance of cyberspace.[21] Applying international relations regime theory to multistakeholder internet governance, Joseph S. Nye Jr. describes the constellation of institutions, rules, laws, policies and norms as a "cyber regime complex," far more distributed and fragmented of an approach than the historical multilateral treaties of space (Nye 2014). In the context of the OST in the mid-1960s, two superpowers dominated space. The number of space-faring nations has grown significantly over the decades.

While space *governance* has continued to centre on the nation-state, a feature that both space and internet *technical architecture* contexts now share is rising privatization. In the same way the internet shifted from the government-funded ARPANET to a commercial global network, space exploration — however nascent — has expanded to private, often billionaire-financed companies such as Blue Origin, SpaceX and Virgin Galactic. The Soviet Union and US "space race" during the Cold War was driven largely by these nation-states, although carried out via private contractors. The internet has had a shift from public funding to private enterprise, and the trajectory of space travel and exploration has begun to shift from the 1960s Manhattan Project-style quest to land a person on the Moon to an era of private exploration.

Major space exploration countries acknowledge and celebrate this privatization of space innovation. For example, the National Space Policy of the United States lists as its first goal to "promote and incentivize private industry to facilitate the creation of new global and domestic markets for United States space goods and services, and strengthen and preserve the position of the United States as the global partner of choice for international space commerce" (The White House 2020, 5). The major space treaties predate this degree of privatization, although the treaties certainly convey state responsibility for all national space activities.

As a Wilson Center article on space governance suggested, "The current global space governance framework has been slow to take evolving state and industry practices as well as technological

20 See www.spaceforce.mil/About-Us/FAQs/Whats-the-Space-Force/.

21 There are many models and many contexts of multistakeholder governance. Drawing from John Ruggie's pioneering study of multilateralism, Mark Raymond and Laura DeNardis (2015) offer a taxonomy of different types of multistakeholder institutional forms that vary based on what combination of actor class is participating, as well as the nature of the authority relations among these actors.

changes into consideration, namely around issues of celestial resource use and space militarization. The growing number of non-traditional players warrants a need for additional, if not revised, legal measures to ensure stronger global space governance and the safety and sustainability of space for the future ahead" (Goguichvili, Linenberger and Gillette 2021).

Beyond the major UN space treaties, there are also more recent, still nation-state-centred, efforts toward bilateral or multilateral agreements and norm development relative to the space domain. The Artemis Accords is one such multilateral agreement. The Artemis Accords is a non-binding, multilateral[22] set of principles for the Artemis human space and exploration program led by NASA and partners — the Canadian Space Agency (CSA), ESA and the Japan Aerospace Exploration Agency (JAXA) — to send astronauts back to the Moon. The Artemis Accords, while an extrapolation of many OST principles, notably includes a section on interoperability: "The Signatories recognize that the development of interoperable and common exploration infrastructure and standards, including but not limited to fuel storage and delivery systems, landing structures, communications systems, and power systems, will enhance space-based exploration, scientific discovery, and commercial utilization. The Signatories commit to use reasonable efforts to utilize current interoperability standards for space-based infrastructure, to establish such standards when current standards do not exist or are inadequate, and to follow such standards."[23]

The ISS helped demonstrate the utility and need for interoperability among space components built by different constituencies. The Artemis Accords speaks to interoperability among lunar bases as they develop, and includes communication standards as a key component of this interoperability. However, note that China is not a signatory. Beyond the practical considerations and shared benefits of making systems interoperate on and around the lunar surface, the existence of technical standards would arguably lower barriers to entry for emerging space-faring nations and companies and increase the sustainability of networks, once developed.

More specific existing space governance tasks related to communication systems also emanate from governmental agreements and coordination. For example, electromagnetic spectrum allocation and non-interference is an important area of international coordination in space. The International Telecommunication Union (ITU), a specialized agency of the United Nations, is responsible for coordination and ensuring non-interference of satellite frequency bands, under the authority of the international Radio Regulations treaty. The ITU is also where orbital slots, essentially the orbital positions, for satellites are assigned.[24]

Principles and norm-setting activities in various areas are also part of the broad space governance framework. Two UNGA resolutions address principles relevant to space communication technologies, albeit geared pragmatically toward communications between Earth and space rather than a network in deep space. These include the Broadcasting Principles (1982) and the Remote Sensing Principles (1986) — the former addressing "use by States of artificial Earth satellites for international direct television broadcasting"[25] and the latter laying out "principles relating to remote sensing of the Earth from space."[26] Norm-setting and standards relevant to ICTs in space cover a diversity of other ad hoc areas such as best practices for commercial rendezvous and proximity operations, sustainability, and other guiding principles and standards developed by organizations such as the International Organization for Standardization (ISO), the Consortium for Execution of Rendezvous and Services Operations, and the Space Safety Coalition, among others.

Satellites have also become the subject of norm-setting commitments to refrain from direct-ascent missile tests. The United States announced in April 2022 its commitment to refrain from conducting

22 As of April 2023, the signatories of the Artemis Accords include Australia, Bahrain, Brazil, Canada, Colombia, France, the Isle of Man, Israel, Italy, Japan, Luxembourg, Mexico, New Zealand, Nigeria, Poland, South Korea, Romania, Rwanda, Saudi Arabia, Singapore, Ukraine, the United Arab Emirates, the United Kingdom and the United States.

23 *Artemis Accords*, 13 October 2020, s 5, online: <www.nasa.gov/specials/artemis-accords/img/Artemis-Accords-signed-13Oct2020.pdf>.

24 For a detailed description of ITU responsibility and also satellite governance more broadly, see Morozova and Vasyanin (2019).

25 *Principles Governing the Use by States of Artificial Earth Satellites for International Direct Television Broadcasting*, GA Res 37/92, UNGAOR, 37th Sess (1982), online: <www.unoosa.org/oosa/en/ourwork/spacelaw/principles/dbs-principles.html>.

26 *Principles Relating to Remote Sensing of the Earth from Outer Space*, GA Res 41/65, UNGAOR, 41st Sess (1986), online: <www.unoosa.org/oosa/en/ourwork/spacelaw/principles/remote-sensing-principles.html>.

direct-ascent ASAT, kinetic-energy missile tests and seek "to establish this as a new international norm for responsible behavior in space" (The White House 2022). Shortly thereafter, a number of countries committed to follow suit, including Canada, Germany, Japan, New Zealand, South Korea and the United Kingdom. Shortly thereafter, the UNGA adopted a draft resolution, "Destructive direct-ascent anti-satellite missile testing" (document A/C.1/77/62), by a vote of 155 for, nine against and nine abstaining, calling "on all States not to conduct such tests and to continue discussions to develop further practical steps and contribute to legally binding instruments on the prevention of an arms race in outer space" (United Nations 2022). The states voting against the resolution were Belarus, Bolivia, Central African Republic, Cuba, Iran, Nicaragua, the Russian Federation and Syria.

These ASAT missile bans are not legally binding, at least as of this writing. But, whereas other security threats in the cyber realm have challenges with attribution, an easily seen and tracked direct-ascent attack on a communication satellite would have clearer attribution. These non-binding agreements also use very specific language around "kinetic" tests, meaning physical missiles striking a target, leaving potentially open other types of attacks. As Aaron Shull, Wesley Wark and Jessica West (2023) explain in their introduction to the CIGI essay series Cybersecurity and Outer Space: "The expansive and non-kinetic nature of harmful cyber activities in space means that they are generally considered below the threshold of warfighting. Yet 'below threshold' does not mean unimportant or lacking in danger."

As the UN Open-Ended Working Group (OEWG) on reducing space threats through norms, rules and principles of responsible behaviours continues its work, it similarly focuses on voluntary, non-legally binding approaches and multilateral space securitization issues such as disarmament and arms race in space, among other space governance topics. Non-kinetic attacks "such as cyber, electronic jamming, and directed energy or lasers" are part of the OEWG discussions (West 2023, 9).

RAND's 2021 report, *Responsible Space Behavior for the New Space Era: Preserving the Province of Humanity*, explains that "Defining rules and norms for the responsible use of space has been a complicated and contentious issue that has been heavily influenced by national security interests over safety," and that has to expand in the contemporary context to safety issues such as space traffic management, debris mitigation and ASAT testing, among other physical safety concerns (McClintock et al. 2021, 5).

Applying and interpreting the rules of international law to the space domain, as Shull and Timiebi Aganaba (2023) explain, is already contentious and "almost always informed by geopolitical strategy, and strong states will interpret existing rules, or influence the creation of new ones, in a manner that benefits their geostrategic interests."

Despite the critical importance of networks in space — both for space applications and critical systems on Earth — there are primarily space governance treaties that predate the modern internet, along with a patchwork of multilateral agreements, principles and norm-setting activities that explicitly address ICT policy in deep space. The next section examines ways in which space governance might adapt to more directly and expansively include the internet governance domain.

A Framework of Multistakeholder Internet Governance in Space

Terrestrial internet governance is not "one thing" but rather an ecosystem of design and coordination functions. In 1999, Larry Lessig's article, "The Law of the Horse: What Cyberspace Might Teach," respectfully suggested the role of code in constituting rights in cyberspace, as well as laws, norms and markets, and how there is nothing to guarantee the politics constructed by that code. What is often overlooked in international treaties, laws and norm-setting is this policy-making role of arrangements of technical architecture. Taken together, the collectivity of design, coordination and oversight functions running the internet on Earth is usually referred to as "distributed, multistakeholder

Internet governance,"[27] a topic addressed by an enormous and venerable body of scholarship.[28]

To examine the applicability and complexity of these functions in deep-space networks, this section uses as a lens a layered framework of terrestrial internet governance taken from the author's work, including from *The Global War for Internet Governance* (DeNardis 2014) and *Researching Internet Governance: Methods, Frameworks, Futures* (DeNardis et al. 2020), among other articles and books.[29] These six layers are:

- administration of critical internet resources (CIRs);
- setting internet standards;
- cybersecurity governance;
- interconnection agreements;
- the policy role of private intermediaries; and
- government regulation and policies.

This section focuses on the first four of these layers because they specifically address technical design and governance areas not substantially addressed in space governance frameworks and because in space they so directly entangle with the other two layers. An examination of these layers can help inform the possible trajectory of governance of an interplanetary internet.

Administration of CIRs

The internet, as designed, requires unique identifiers and so too will an interplanetary internet require a name and number space. In the terrestrial internet, these CIRs primarily include domain names, Internet Protocol (IP) addresses, autonomous system numbers (ASNs) and a variety of unique protocol numbers. Domain names are the globally unique, human-readable, alphanumeric identifiers assigned to websites and other virtual resources. IP addresses are the unique binary numbers assigned uniquely, even if just for a session, to a device using the internet.[30] The internet is a network of interconnected networks, technically called autonomous systems. ASNs are globally unique binary numbers assigned to these networks. Whether owned by a telecommunications provider such as AT&T, a large media company such as Google or a content distribution network such as Akamai, they each have a unique binary number that aids in interconnection among networks.

This description of CIRs is oversimplified but serves to make the point that unique virtual identifiers are necessary for information to reach its destination over a network. Because each identifier on Earth has to be globally unique, someone has had to manage the distribution and use of these identifiers. But there are many other governance functions necessary to keep this entire system running: assigning domain names, allocating and assigning IP addresses, assigning protocol numbers, resolving DNS queries, operating root servers for each domain, authorizing changes to the root zone file, managing the root zone file, resolving domain name trademark disputes, securing the DNS, authorizing the use of new language scripts in the DNS and adjudicating domain name trademark disputes.

The institutions that carry out these tasks are similarly varied, including the Internet Corporation for Assigned Names and Numbers (ICANN) and its Internet Assigned Numbers Authority (IANA) functions; DNS registries; domain name registrars that assign names; domain name dispute resolution providers that resolve trademark disputes; and regional internet registries (RIRs) such as the African Network Information Centre, the Asia-Pacific Network Information Centre, the American Registry for Internet Numbers, the Latin American and Caribbean Network Information Centre, and Réseaux IP Européens Network Coordination Centre (RIPE NCC) in Europe, the Middle East and Central Asia. Very little of this is controlled by governments in the contemporary context, in part because of

27 On the topic of multistakeholder internet governance, see Hofmann (2020); Raymond and DeNardis (2015).

28 On the policy-making role of private industry, see, for example, MacKinnon (2011); Klonick (2018). On the role of multistakeholder technical coordinating institutions, see, for example, Mueller (2002); Klein (2002); Kleinwächter (2000). On the role of international organizations, see Levinson and Marzouki (2015). On the role of technical design, see Braman (2011); Ermoshina and Musiani (2022). On the role of governments in internet governance, see, for example, Van Eeten and Mueller (2013); Goldsmith and Wu (2006).

29 See, for example, DeNardis (2013).

30 There are two types of IP addresses: the historic Internet Protocol version 4 (IPv4) that assigns 32 bits (0s and 1s) to each address for a total IP address space of 2^{32} or roughly 4.3 million unique addresses; and Internet Protocol version 6 (IPv6), the standard that dramatically increases the available pool of IP addresses by assigning 128 bits to each address for a total IPv6 address pool of 2^{128} or 340 undecillion available addresses (picture 340 followed by 36 zeros).

how the structures have evolved over time. In the same way, government involvement in the early coordination of space CIRs may follow suit.

A solar-system internet will have commensurate requirements for unique identifiers, for addressing of nodes, data, regions and eventually for network domains, among others. What will be the equivalent of IP addresses, protocol numbers and ASNs in space? For example, some leading early architectural efforts to design delay- and disruption-tolerant protocols for deep-space environments indicate that IP addresses will be replaced by, or complemented by, Bundle Protocol addresses.

Because of the expansiveness of space and multiple competing design efforts, it is not preordained that there will be a universal address space. Universality is a design choice and an issue of institutional cooperation.

Another open governance question is whether the institutional complex overseeing the allocation and assignment of unique identifiers on Earth (i.e., ICANN, IANA, RIR, and so forth) will extend into space. This is a consequential question because it relates to the issue of whether there will be interoperability between the classical internet and solar-system networks. Already, there is an effort of completely distinct institutional jurisdiction materializing for space numbers. For example, the Consultative Committee for Space Data Systems (CCSDS), formed by the world's major space agencies (including JAXA, ESA, NASA, CNSA, CSA and others) in 1982 to develop standards and solve common problems for space data systems, has established the Space Assigned Numbers Authority to register protocol identifiers and other standards-related identities (CCSDS 2020a).

Another CIR governance function in deep space, and one requiring international coordination, is the allocation of electromagnetic spectrum and orbital slots. For satellites orbiting the Earth, orbital slots refer to the geostationary orbit (i.e., locations) at which satellites/spacecrafts are authorized to remain and operate. Radio-frequency spectrum, which similarly requires allocation coordination to avoid interference, is a finite resource necessary for satellite (and other wireless) communication. This could follow directly from near-Earth regulations and oversight. Coordination of these two functions, carried out by the UN specialized agency for telecommunications (the ITU), is necessary to circumvent interference.

The ITU Radio Regulations is an international treaty with governance authority over a relevant portion of electromagnetic spectrum.[31] The logic of this coordinating function extends to outer space, including inter-satellite communications.

It is less certain whether the DNS resolving names into numbers will extend into deep space, at least as currently designed. The back and forth of DNS query lookups may not be tenable over astronomical distances because of the latency involved. A domain name lookup that takes an hour is not acceptable in any context, and objects could have moved in the interim. In the long term, any system resolving names into numbers would either have to take place in a highly localized, store-and-forward approach, or be redesigned to reduce back-and-forth transmissions.

The logic of coordinating and oversight functions for terrestrial and near-Earth internet governance will extend into space. Someone will have to assign unique identifiers and coordinate everything from deep-space orbital slots to unique numbers assigned to nodes, networks, data, sensors, actuators and regions of space. Some CIR governance functions in space reside far into the future, such as dealing with the space equivalent of domain name trademark disputes and whether a DNS function is needed at all. The question of how these identifiers are allocated, by whom and under what process, will likely be as economically and politically important and possibly as contentious as control of CIRs on Earth. Box 1 seeks to summarize some first-round CIR governance areas for an interplanetary internet.

Setting Standards for an Interplanetary Internet

The design of technical standards is a core function of internet governance involving the creation of interoperability blueprints for all dimensions of digital information exchange, including encryption, error detection and correction, formatting, authenticating, encoding, addressing, routing, interconnection and more. Prior to the development of open internet standards such as Transmission Control Protocol/Internet Protocol (TCP/IP), networks connecting devices made by one company, such as Apple, were unable to easily

31 The 2020 edition of the ITU Radio Regulations is available at www.itu.int/pub/R-REG-RR-2020.

Box 1: First-Round CIR Governance for a Solar-System Internet

- **Name and number space design:** designing the name and number space (or spaces) for identifying nodes, networks, data, sensors, actuators and regions.
- **Identifier assignment process:** creating a process for allocating, assigning and distributing unique identifiers.
- **Institutional authority for name and number allocations:** selecting an institution or system of institutions responsible for coordinating unique identifiers.
- **Satellite resource allocation:** allocating electromagnetic frequency and orbital slots in deep space.
- **Time standard:** selecting and coordinating a time standard or standards across celestial bodies.
- **Name and number translation:** possibly redesigning a DNS-like function that is delay and disruption tolerant.

communicate with networks connecting devices made by another company, such as IBM. Each network used proprietary standards that were closed to other innovators. The core standards of the terrestrial internet, perhaps more than anything else, are what created the universal internet that is accessible from anywhere around the world and that serves as a substrate for applications as far ranging as the World Wide Web, video streaming, voice calls and online financial services.

In order for an interplanetary internet to become a similar substrate for future applications and innovations not yet imaginable, it would similarly have to be built upon open standards that create interoperability, competition and universality. In space, as on Earth, there will also be tensions between the need for this openness and the need for protected and closed systems, whether for national security purposes or national economic advantage. For many future applications and maximum human benefit, interoperability with the terrestrial internet is necessary. Given the need to redesign technology to meet unique space conditions and given political tensions between major spacefaring nations, achieving this interoperability may face challenges.

There is not "one protocol" that standardizes the internet but countless, such as Wi-Fi, Bluetooth, Hypertext Transfer Protocol Secure, Secure Sockets Layer, TCP/IP, BGP, Joint Photographic Experts Group, Moving Picture Experts Group, Voice over Internet Protocol, IPv6, H.323, Internet Protocol Security, Transport Layer Security, Domain Name System Security Extensions, IPv4, American Standard Code for Information Interchange, Unicode, near-field communication, Pretty Good Privacy (PGP), Simple Mail Transfer Protocol, OpenPGP, 6in4, Real-time Transport Protocol, Internet Message Access Protocol and countless others. The IETF, responsible for establishing core internet protocols and making them openly available via the Request for Comments (RFC) series, is one of numerous standards-setting institutions developing specifications for digital technologies. Some of these include the World Wide Web Consortium, ISO and the Institute of Electrical and Electronics Engineers, among many others.

A solar-system internet will also not be built upon one single standard but a constellation of standards that address various requirements. Because of the unique space requirements outlined in the first section, this architecture will not simply be a replication of the classical internet. The core networking standards of the internet require significant adjustments to accommodate the unique conditions in deep space such as signal delay and environmental disruption.

Standards efforts are under way to develop delay-tolerant network architectures (Cerf et al. 2007). IETF engineers working in the Delay-Tolerant Networking Research Group of the Internet Research Task Force have been developing protocols designed to address constant network interruptions, such as by introducing persistent storage on network nodes and building in both diagnostic and management features designed to provide network reliability and stability. As RFC 9171 explains, "Delay-Tolerant Networking is a network architecture providing communications in and/or through highly stressed environments. Stressed networking environments include those with intermittent

connectivity, large and/or variable delays, and high bit error rates" (Burleigh, Fall and Birrane 2022).

A separate standardization effort is under way in the CCSDS of ISO. The committee has developed many technical specifications for information systems in space.[32]

An open governance question is whether the core standards under way for space networks are encumbered with standards-based patents, a concern with implications for innovation, competition and also the question of change control over standards in the future.

At a higher level of standards governance, the larger question is what institution becomes the authority for developing standards for an interplanetary internet (see Box 2). In the terrestrial digital ecosystem, there are multiple standards-setting institutions focusing on different aspects of standardization, with the IETF developing core internet standards. At the early stage of design, there are arguments for multiple organizations in innovation competition. There are also important rationales for cooperation and bringing together expertise from different design communities. As an Interplanetary Networking Special Interest Group report rightly expresses in the context of dual efforts in the IETF and the CCSDS, "There is an open question regarding the management authority of the standards: which standards organization is the proper authority for developing and publishing standards and ensuring that implementations conform to them?" (Kaneko et al. 2021, 28).

Cybersecurity Governance

Securing the core, common infrastructure underlying all digital transactions remains one of the most critical functions of internet governance. This includes securing systems of routing; securing the DNS; authenticating websites using public key cryptography and trusted third-party certificate authorities; defending critical internet sites against distributed denial of service attacks, viruses, worms, disruptions, ransomware, and unauthorized eavesdropping and use; and authenticating handoffs among network operators. The design, implementation, coordination and regulation of internet security span multiple institutions, both private and public.

Box 2: First-Round Standards Governance for an Interplanetary Internet

- **Standards architectures:** developing delay-tolerant technical standards for formatting, encoding, compression, error detection and correction, encryption, addressing, and so forth.
- **Procedural openness:** assessing the standards-development processes for participatory openness, due process, transparency, public document availability and other characteristics legitimizing technical expertise-based governance.[31]
- **Standards harmonization:** once working standards emerge, assessing opportunities for harmonization across relevant institutions and with the classical internet.
- **IPR:** establishing policies and norms about standards-based patents, reasonable and non-discriminatory access, and open standards.
- **Government procurement policies:** selecting standards for initial government investments in space networks.
- **Interoperability agreements:** establishing voluntary communication interoperability agreements among government space programs.

Space communication technologies have already become, in practice, part of critical infrastructure, necessary for vital transactions and services on Earth and part of the apparatus of national security. The security requirements for the classical internet all extend into the critical space domain: confidentiality and integrity of information; strong authentication of nodes; protection from attack; and trusted handoffs among networks.

32 To gain a sense of this work, see, for example, CCSDS (2020b).

33 As Corinne Cath (2023, 8) elaborates, there can also be a "disconnect between procedural openness and actual accessibility," rooted in culture, as well as economic and technical barriers to participation.

An open question is whether to build in a stronger identity system to authenticate who is using the solar-system network, an attribute that would facilitate attribution and accountability, on one hand, but raise privacy and speech questions, on the other. Trust and security architectures trailed the commercialization and global reach of the internet. It is possible that a deep-space network will have a security advantage in that strong security can be engineered in from the beginning. But a crucial design concern for strong encryption and authentication — whether via public-key cryptography, emerging blockchain frameworks, quantum-resistant algorithms or another approach — is the requirement for working over long distances. Governments have historically tried to weaken encryption to carry out surveillance, intelligence, counterterrorism and law enforcement functions. The same tensions among sometimes conflicting values — critical infrastructure security versus intelligence gathering, for example — will extend to space, only with additional sovereignty complexities.

Many institutional forms of cybersecurity governance[34] could have important applications in space. Computer emergency response teams (CERTs) or computer security incident response teams (CSIRTs) are public-private institutions that notify the public of software vulnerabilities, cybersecurity incidents and the need for updates. They pass along security bulletins from the private sector and information about mitigating vulnerabilities. A CERT devoted to space-cyber vulnerabilities, incidents and responses is a novel and possibly important idea as space networking evolves.

Certificate authorities are another category of internet governance institution that could be critical for a solar-system internet. These trusted third parties vouch for the digital certificates necessary for public-key cryptography, certifying identities, information, websites and networks. This area is as problematic as it is important. A fundamental governance question is what makes these third parties trustworthy enough to perform this function. A system of trusted third-party digital signature verification for space may face similar challenges, but is essential for creating the requisite trust architectures.

Concerns about cyberwar and cybersecurity attacks carried out by a multitude of players, regrettably, also will convey into space. Carrying out deception, intelligence gathering and surveillance, and disruptions in space will be part of the cyberwarfare domain. Discussions about responsible state behaviour in space usually focus on physical attacks. Even when discussing satellites, the focus is often on kinetic attacks. Whether or not this is intentional, this leaves out virtual attacks of all kinds (see Box 3). Cyberattacks can achieve the same effects of taking down satellites or causing commensurate disruptions. An open governance question is whether nation-states will agree to refrain from cyber disruptions.

Box 3: First-Round Cybersecurity Governance for a Solar-System Internet

- **Delay-tolerant security architecture:** establishing protocols for a comprehensive trust architecture.
- **Space CERT:** establishing a public-private CERT or CSIRT focused on space networking.
- **Certificate authority for space:** developing a trusted third party certifying digital signatures in space, including for information integration and authenticating nodes and networks.
- **Interconnection security:** securing handoffs between networks.
- **Cybersecurity treaties/agreements:** agreeing to refrain from governmental cyber-offensive attacks on a solar-system internet and stockpiling of known vulnerabilities.
- **Identity infrastructures:** designing appropriate identity systems for nodes, networks and possibly for those accessing the network.
- **Space communication as critical infrastructure:** where not already specified, incorporate space communication networks into larger critical infrastructure protection policies.

34 For a detailed account of cybersecurity governance, see DeNardis (2014, chapter 4).

Interconnection Agreements

Although the internet is metaphorically described as a "cloud," it is, of course, a network of networks. These networks do not just connect. They are deliberately interconnected via technical protocols, physical interconnection, and largely private contractual agreements among network operators to conjoin their networks either bilaterally or at IXPs. This is a highly privatized area involving both physical and logical connections and business agreements to exchange packets between autonomous systems. On Earth, the types of businesses interconnecting are network providers, large content companies and content delivery networks. Because decisions to interconnect are usually privately negotiated, this is an internet governance area with little transparency. In general, these agreements to exchange information can involve settlement-free peering, paid peering or paid transit agreements in which one operator pays another to exchange traffic. There is not considerable regulatory oversight of these interconnection agreements, or of IXPs, and they raise public policy concerns about competition, antitrust, points of disruption and surveillance, and digital inclusion.[35]

Networks are able to interconnect to form the global internet because of the common use of an inter-domain routing protocol called BGP. This protocol allows each autonomous system to exchange a complete accounting of routing information, or what resources are reachable via their networks. The historic basis of this structure is trust among networks and, as the internet has evolved, BGP and interconnection have become a vulnerable part of digital infrastructure (Fraire 2017, 124–27). False routing information injected into the system has caused disruptions, deceptions and outages, and resulted occasionally in rerouting of transmissions through faraway countries, whether accidentally or from a politically motivated act. Ongoing efforts to secure interconnection via public key cryptography have been under way, but raise difficult infinite regress questions around trust such as what trusted third party should validate these encryption keys.

The interplanetary internet will also be a network of networks, with the same governance and coordination requirements — securing and authenticating exchanges, agreeing on interoperability standards, establishing financial terms for interconnection — along with many, many more complications. Perhaps more than any other area of internet governance, there are stunning technical and political differences between interconnection on Earth and in deep space, even beyond the shift from a constellation of physical fibre optic, twisted pair, and coaxial cable and wireless (cellular, microwave, Wi-Fi and satellite) approaches, to entirely wireless transmission, including both radio-frequency and optical communication. Governments with advanced space programs, or public-private partnerships, rather than private businesses will likely make these initial investments. A more consequential shift is that interconnection needs to assume intermittent and variable connectivity. All objects are continuously moving relative to each other, causing connectivity variability and disruptions beyond outages from exogenous natural (solar flares, micrometeoroid) and human-made (orbital debris) factors.

Deep-space interconnection needs to account for relative positional movement and intermittent disruptions, requiring store-and-forward capability but also continuous predictive information about when devices are positionally capable of communications. Rather than assuming always-connected interconnection, whether bilaterally or at multi-network exchange points, interconnection will require "contact plan" information about "episodes of communications" or simply "an opportunity to establish a temporal communication link" (ibid.). Procedures and institutional responsibility for developing these contact plans will be a critical new governance function.

It cannot be assumed that national space program networks or private-public partnerships will have incentives to interconnect their networks because of national security, mission safety and other concerns. But if they do not, whether through radical air-gapping of networks or the use of closed proprietary specifications rather than shared standards, the ensuing networks will emulate the proprietary systems of the twentieth century rather than a public-purpose, multi-use solar-system network for shared discovery and exploration. Engineering and coordinating high systems of interconnection security — even if within multiple independent networks — is a prerequisite for interconnection progress (see Box 4).

35 For a detailed account of interconnection architecture and policy, see DeNardis (2014, chapter 5).

Internet Governance Flashpoints Applicable in Space

Deep-space exploration and discovery will not exist without a reliable communication network that is multipurpose, interoperable and secure. While this paper has sought to suggest a layered framework of internet governance decisions likely applicable to deep space, it can also be assumed that many of the controversial internet governance flashpoints on Earth will also extend into space in the next half century. Drawing from the history of internet governance themes and controversies, the following are anticipated flashpoints that could help inform interplanetary internet governance.

Conflicts Will Likely Emerge Over Control of a Common Addressing Scheme

IP addresses such as the IPv4 address 11000000 01010001100000111010000 1, usually written in shorthand dotted-decimal notation such as, for this address, 192.81.131.161, seem as uncontroversial as imaginable. Yet control and oversight of internet addresses and other critical resources have arguably been as historically contentious as more obviously political issues such as government censorship and surveillance. The so-called IANA functions allocating unique addresses were once carried out by a single individual, Jon Postel, before evolving into an institutional system eventually around ICANN with oversight by the US Department of Commerce. After years of global debate, and with some American politicians describing the transition as America's internet surrender, the functions transitioned to the ICANN-administered system. The technological affordances of unique identifiers — criticality, finite resources, global uniqueness — somewhat explain the attending controversies. IP addresses are necessary for nearly all social, economic and political transactions over digital networks, hence the political and economic interest in control of the finite pool of these resources, metaphorically or pragmatically. These identifiers, because of the requirement of global uniqueness for each session, have also morphed into personal identifiers, at least when combined with other information such as that provided by a network operator. IP addresses, and certainly the DNS, have also become a site of filtering and blocking. IP continues to be politicized, including movements from China to create a "new IP."

These same types of control struggles and politicization of addressing — including the question of whether there even will or should be a common addressing system across adversarial states — should be anticipated for the CIRs and unique identification systems in a solar-system internet.

Box 4: First-Round Interconnection Governance for a Solar-System Internet

- **Inter-domain routing design:** design of a BGP-like standard for exchanging information among space domains and networks.
- **Interconnection security governance:** development of a certificate authority technical plan and institutional structure for authenticating nodes and reachability information.
- **Network identification architecture:** related to CIR recommendations above, i.e., establishment of a unique numbering system for identification of space networks, regions or segments.
- **Peering agreements:** establishing agreements for exchanging information, similar to peering and transit contracts in the terrestrial internet, including government agreements on interconnection of mission-related networks.
- **Contact plans:** a technical and institutional procedure for calculating, developing and disseminating "contact plans," the temporal and spatial opportunities for communications between moving and intermittently connected objects.

Interoperability, Including with the Classical Internet, Is Not Preordained

The architecture of an interplanetary internet will be novel because of the technical constraints and unique contexts of space, such as delay and disruption tolerance. Creating interoperability with the classical internet is not at all preordained, but something that has to be designed. Without this backward compatibility, the discovery, education, commercial and exploration benefits of space networks will be more limited. Challenges implementing IPv6 on Earth ensued because of the lack of backward compatibility between IPv4 and IPv6, as well as other complicating factors.[36] Building native Earth-space interoperability into the completely redesigned architectures may be infeasible because of the many necessary space adaptations, so translation mechanisms and other technological bridges will likely be necessary for achieving interoperability.

Avoiding Fragmentation Requires Standards Harmonization

Other rapidly emerging internet landscapes, such as around the IoT and quantum-resistant communication technologies are, to various degrees, fragmented and carried out by multiple competing standards institutions doing the same work.[37] The standards landscape materializing around networks in space may be similarly heterogenous and fragmented. While this competition and incompatibility may be inevitable, and even helpful, for maximizing innovation in the contemporary moment, avoiding fragmentation and incompatible networks (and duplicative investment) later requires some international coordination and harmonization, possibly incentivized by government procurement policies or security frameworks.

Change control struggles over standards, and tensions around institutional authority over standardization, have been a recurrent theme in internet governance, certainly since the 1990s tensions between the Open Systems Interconnection (OSI) protocols and the TCP/IP suite that would form the basis of the global internet. It is worth noting that the two key standards communities involved in these historic efforts, the IETF and ISO, are also involved in current efforts to develop space network protocols.

Open Standards Are Necessary Now for Private Investment Later

The availability of open standards — openly developed, openly published and unencumbered by standards-based patents — has contributed to the rapid growth and innovation around the global internet.[38] Yet there has always remained a tension between this openness and proprietary enclosure, whether in social media services, hardware or the IoT. The private investment eventually necessary for the development, adoption and use of a solar-system internet will depend, in part, upon architectural openness, the assurance that a software or hardware product developed will interoperate with other products or that a network will interoperate with another network. Historically, open standards have shaped economic competition and inclusion. If different solar-system networks are based on IPR-encumbered standards, or completely closed unpublished specifications, there will likely not be competitive investment in a solar-system internet.

Standardization Does Not Assure Implementation or Usage

Internet history is replete with examples of widely touted standards that were never adopted into product development or widespread usage. The highest-profile example of this may be the OSI protocol suite that many governments and businesses considered a solution to moving from proprietary network architectures to universal interoperability. Instead, the TCP/IP standards emerged as the foundational basis for interoperability from the principle of rough consensus and working code.[39] Standards are blueprints. To be used, they require proven concepts, implementation in products and also adoption. As various concurrent efforts at space standardization continue, history suggests that some may never translate into implementation and use.

36 For a detailed account of the design, development and governance of IPv6, see DeNardis (2009).

37 See, for example, DeNardis (2020, chapter 5).

38 For a detailed account of open standards and global interoperability, see DeNardis (2011).

39 For one account of the history of TCP/IP versus OSI, see Russell (2014).

Technical Governance in Space Will Become Highly Politicized

Because technical design often makes public policy decisions, and because of the security and economic stakes of deep-space networking, design efforts will likely be politicized. This has happened throughout the development of digital technologies. Encryption architectures, and especially encryption key strength, have remained at the centre of conflicts between the public policy goal of securing critical infrastructure and the objective of weakening encryption for law enforcement and intelligence functions. Part of the essential tension exists between cyber offence and defence. Should space networks be "air gapped" or should they inherently be interoperable and overlaid with tight security? All of the cyberwar tensions that exist on Earth, such as governmental calculations about when to stockpile zero-day exploits for cyber offence versus when to disclose them to increase cybersecurity, will also exist in space. So too will critical debates about environmental concerns and natural resources that directly connect to and extend into space contexts.

The tension between multilateral and multistakeholder models of governance will also leap into space. Throughout internet history, there have been incommensurable world views about technology governance and especially tensions between cybersovereignty approaches versus more distributed models. Because national space programs are leading initial investments in space networking, and because of inherent competition among national space programs, this tension between so-called cybersovereignty versus multistakeholder governance can be expected. The strange distinction between cyber and internet on Earth, which makes little engineering sense because the technical architecture is the same, will likely carry over into space, with one group primarily focused on national security and cyberwar.

Infrastructures of Internet Governance in Space Will Be Co-opted as a Proxy for Political Power

In the same way the DNS is regularly co-opted by governments and companies for content control, such as carrying out political censorship or enforcing IPR, so too might infrastructures of internet governance in space be co-opted as a proxy for heliopolitical power. Governments turn to infrastructure companies and coordinating institutions (hosting services, network operators, platforms, domain name registries) to carry out everything from disruptions to surveillance. In the immediate aftermath of the Russian invasion of Ukraine, the Ukrainian deputy minister of digital transformation asked both ICANN and RIPE NCC (the relevant regional internet registry) to essentially disconnect Russia from the internet.[40] The institutions declined to do so for a variety of technical and procedural reasons. Because of the *sui generis* strategic importance of space networks and also the strategic importance of space networks to national security, societal functioning and the economy on Earth, emerging space networks will also become a target for carrying out political objectives having nothing to do with the networks' original operational mission. This historic pattern in internet governance emphasizes the need for international cooperation and treaties around space networks, as well as strong cybersecurity to mitigate against politically motivated disruptions and other interventions.

40 Mykhailo Federov to Goran Marby, February 28, 2022, www.icann.org/en/system/files/correspondence/fedorov-to-marby-28feb22-en.pdf; Mykhailo Federov to Hans Petter Holen, March 2, 2022, www.ripe.net/publications/news/announcements/request-from-ukrainian-government.pdf.

Entangling Space Governance and Internet Governance

In the same way technology constantly evolves, so too must technology governance evolve. This paper has explored some unique constraints of space that will shape interplanetary internet governance, assessed the relevance of international space treaties to deep-space networks, suggested an initial layered framework of internet governance applicable in space, and closed with some terrestrial internet governance themes that might help inform nascent structures and efforts around interplanetary internet governance.

The communities involved in space governance writ large are not the same communities involved in internet governance, so a first step is to bring these expert communities into conversation. The internet is making a leap off Earth into outer space. Space governance frameworks must evolve to incorporate internet governance. So too must internet governance evolve to meet the space moment.

Acknowledgements

The author gratefully acknowledges the feedback and insights from Tarah Wheeler, Fiona Alexander, Anupam Chander and participants in the Tech Law Colloquium at Georgetown Law School, Eli Noam and fellows of the Columbia Institute for Tele-Information, Scott Pace, Samantha Bradshaw, Corinne Cath, Niels ten Oever, Mark Raymond, Aaron Shull, Nanette Levinson, Oscar A. Garcia Malnero, James Schier, Scott Burleigh, Michael Snell, Yosuke Kaneko, Francesca Musiani, Ben Compaine, Michael Nelson, Evan Barba, Leticia Bode, Meg Leta Jones, Micha Koliska, Michael Macovski, Martin Irvine, Emily Tavoulareas, Jeanine Turner and generous anonymous peer reviewers.

Works Cited

Aganaba, Timiebi. 2021. "Innovative Instruments for Space Governance." Opinion, Centre for International Governance Innovation, February 8. www.cigionline.org/articles/innovative-instruments-space-governance/.

Bowker, Geoffrey C. and Susan Leigh Starr. 1996. "How things (actor-net) work: Classification, magic and the ubiquity of standards." *Philosophia* 23 (3–4): 195–220.

Braman, Sandra. 2011. "The Framing Years: Policy Fundamentals in the Internet Design Process, 1969–1979." *The Information Society* 27 (5): 295–310.

Burleigh, Scott, Kevin Fall and Edward J. Birrane. 2022. "Bundle Protocol Version 7: RFC 9171." December 14. https://datatracker.ietf.org/doc/rfc9171/.

Cath, Corinne. 2023. "Loud Men Talking Loudly: Exclusionary Cultures of Internet Governance." Amsterdam, The Netherlands: Critical Infrastructure Lab. April. www.criticalinfralab.net/wp-content/uploads/2023/04/LoudMen-CorinneCath-CriticalInfraLab.pdf.

CCSDS. 2020a. "Space Assigned Numbers Authority (SANA) — Role, Responsibilities, Policies, and Procedures." CCSDS 313.0-Y-3. Yellow Book. Washington, DC: CCSDS. October. https://public.ccsds.org/Pubs/313x0y3.pdf.

———. 2020b. "Space Packet Protocol." Recommended Standard CCSDS 133.0-B-2. Blue Book. Washington, DC: CCSDS. June. https://public.ccsds.org/Pubs/133x0b2e1.pdf.

Cerf, Vinton Gray, Scott C. Burleigh, Adrian J. Hooke, Leigh Torgerson, Robert C. Durst, Keith Scott, Kevin Roland Fall and Howard Weiss. 2007. "Delay-Tolerant Networking Architecture." RFC 4838. April. www.rfc-editor.org/info/rfc4838.

Clark, David D. 2018. *Designing an Internet.* Cambridge, MA: MIT Press.

D'Agostino, Susan. 2020. "To Boldly Go Where No Internet Protocol Has Gone Before." *Quanta Magazine,* October 21. www.quantamagazine.org/vint-cerfs-plan-for-building-an-internet-in-space-20201021/.

DeNardis, Laura. 2009. *Protocol Politics: The Globalization of Internet Governance.* Cambridge, MA: MIT Press.

———, ed. 2011. *Opening Standards: The Global Politics of Interoperability.* Cambridge, MA: MIT Press.

———. 2013. *Internet Points of Control as Global Governance.* Internet Governance Papers No. 2. Waterloo, ON: CIGI. www.cigionline.org/static/documents/no2_3.pdf.

———. 2014. *The Global War for Internet Governance.* New Haven, CT: Yale University Press.

———. 2020. *The Internet in Everything: Freedom and Security in a World with No Off Switch.* New Haven, CT: Yale University Press.

DeNardis, Laura, Derrick Cogburn, Nanette S. Levinson and Francesca Musiani, eds. 2020. *Researching Internet Governance: Methods, Frameworks, Futures.* Cambridge, MA: MIT Press.

Ermoshina, Ksenia and Francesca Musiani. 2022. *Concealing for Freedom: The Making of Encryption, Secure Messaging and Digital Liberties.* Manchester, UK: Mattering Press.

Fraire, Juan A. 2017. "Introducing Contact Plan Designer: A Planning Tool for DTN-Based Space-Terrestrial Networks." In *6th International Conference on Space Mission Challenges for Information Technology (SMC-IT)*, 124–27, Madrid, Spain.

Goguichvili, Sophie, Alan Linenberger, Amber Gillette and Alexandra Novak. 2021. "The Global Legal Landscape of Space: Who Writes the Rules on the Final Frontier?" Wilson Center, October 1. www.wilsoncenter.org/article/global-legal-landscape-space-who-writes-rules-final-frontier.

Goldin, Daniel S. 1999. "Pathway to the Future." *Scientific and Technical Aerospace Reports* 37.

Goldsmith, Jack and Tim Wu. 2006. *Who Controls the Internet? Illusions of a Borderless World.* New York, NY: Oxford University Press.

Guston, David H. 2014. "Understanding 'Anticipatory Governance.'" *Social Studies of Science* 44 (2): 218–42. https://doi.org/10.1177/0306312713508669.

Hofmann, Jeanette. 2020. "The Multistakeholder Concept as Narrative: : A Discourse Analytical Approach." In *Researching Internet Governance: Methods, Frameworks, Futures*, edited by Laura DeNardis, Derrick Cogburn, Nanette S. Levinson and Francesca Musiani, 253–68. Cambridge, MA: MIT Press.

Jasanoff, Sheila. 2016. *The Ethics of Invention: Technology and the Human Future.* New York, NY: W. W. Norton.

Johnson, David R. and David Post. 1996. "Law and Borders: The Rise of Law in Cyberspace." *Stanford Law Review* 48 (5): 1367–402. https://doi.org/10.2307/1229390.

Jones, Andrew. 2022. "Chinese satellite in near miss with Russian ASAT test debris." *Space News*, January 20. https://spacenews.com/chinese-satellite-in-near-miss-with-russian-asat-test-debris/.

Kaiser, Jocelyn. 1998. "Interplanetary Internet." *Science* 281 (5379): 879.

Kaneko, Yosuke, Vinton Cerf, Scott Burleigh, Maria Luque and Kiyohisa Suzuki. 2021. *Strategy Toward a Solar System Internet for Humanity.* Interplanetary Networking Special Interest Group, Strategy Working Group Report. June. https://ipnsig.org/wp-content/uploads/2021/10/IPNSIG-SWG-REPORT-2021-3.pdf.

King, Julia. 2007. "Google's Internet Evangelist Vint Cerf on the Hot Seat." *Computerworld*, July 30.

Klein, Hans. 2002. "ICANN and Internet Governance: Leveraging Technical Coordination to Realize Global Public Policy." *The Information Society* 18 (3): 193–207. https://doi.org/10.1080/01972240290074959.

Kleinwächter, Wolfgang. 2000. "ICANN between technical mandate and political challenges." *Telecommunications Policy* 24 (6–7): 553–63.

Klonick, Kate. 2018. "The New Governors: The People, Rules, and Processes Governing Online Speech." *Harvard Law Review* 131: 1598–1670.

Latour, Bruno. 1992. "Where Are the Missing Masses? The Sociology of a Few Mundane Artifacts." In *Shaping Technology/Building Society: Studies in Sociotechnical Change*, edited by Wiebe E. Bijker and John Law, 225–58. Cambridge, MA: MIT Press.

Levinson, Nanette S. and Meryem Marzouki. 2015. "International Organizations and Global Internet Governance: Interorganizational Architecture." In *The Turn to Infrastructure in Internet Governance*, edited by Francesca Musiani, Derrick L. Cogburn, Laura DeNardis and Nanette S. Levinson, 47–71. New York, NY: Palgrave Macmillan.

MacKinnon, Rebecca. 2011. *Consent of the Networked: The Worldwide Struggle for Internet Freedom.* New York, NY: Basic Books.

McClintock, Bruce, Katie Feistel, Douglas C. Ligor and Kathryn O'Connor. 2021. *Responsible Space Behavior for the New Space Era: Preserving the Province of Humanity.* RAND Corporation. www.rand.org/pubs/perspectives/PEA887-2.html.

Morozova, Elina and Yaroslav Vasyanin. 2019. "International Space Law and Satellite Telecommunications." Oxford Research Encyclopedias, December 23. https://doi.org/10.1093/acrefore/9780190647926.013.75.

Mueller, Milton L. 2002. *Ruling the Root: Internet Governance and the Taming of Cyberspace*. Cambridge, MA: MIT Press.

———. 2020. "Against Sovereignty in Cyberspace." *International Studies Review* 22 (4): 779–801. https://doi.org/10.1093/isr/viz044.

Musiani, Francesca. 2022. "*Infrastructuring* digital sovereignty: a research agenda for an infrastructure-based sociology of digital self-determination practices." *Information, Communication & Society* 25 (6): 785–800. https://doi.org/10.1080/1369118X.2022.2049850.

Musiani, Francesca, Derrick L. Cogburn, Laura DeNardis and Nanette S. Levinson, eds. 2016. *The Turn to Infrastructure in Internet Governance*. New York, NY: Palgrave Macmillan.

NASA. 2007. "Chinese Anti-satellite Test Creates Most Severe Orbital Debris Cloud in History." *Orbital Debris Quarterly News* 11 (2): 2–3. https://orbitaldebris.jsc.nasa.gov/quarterly-news/pdfs/odqnv11i2.pdf.

———. 2019. "Two Break Up Events Recorded." *Orbital Debris Quarterly News* 23 (3): 1–2. https://ntrs.nasa.gov/api/citations/20190028811/downloads/20190028811.pdf.

———. 2022. "The Intentional Destruction of Cosmos 1408." *Orbital Debris Quarterly News* 26 (1): 1–5. https://orbitaldebris.jsc.nasa.gov/quarterly-news/pdfs/odqnv26i1.pdf.

Nye, Joseph S. Jr. 2014. *The Regime Complex for Managing Global Cyber Activities*. Global Commission on Internet Governance Paper No. 1. Waterloo, ON: CIGI. May. www.cigionline.org/static/documents/gcig_paper_no1.pdf.

Pace, Scott. 2023. "U.S. Space Policy and Theories of International Relations: The Case for Analytical Eclecticism." *Space Policy*, January. https://doi.org/10.1016/j.spacepol.2022.101538.

Raymond, Mark and Laura DeNardis. 2015. "Multistakeholderism: anatomy of an inchoate global institution." *International Theory* 7 (3): 572–616.

Russell, Andrew L. 2014. *Open Standards and the Digital Age: History, Ideology, and Networks*. New York, NY: Cambridge University Press.

Shull, Aaron and Timiebi Aganaba. 2023. "Formulating, Interpreting and Applying International Law in Space." Cybersecurity and Outer Space Essay Series, Centre for International Governance Innovation, January 29. www.cigionline.org/articles/formulating-interpreting-and-applying-international-law-in-space/.

Shull, Aaron, Wesley Wark and Jessica West. 2023. "Securing the New Space Domain: An Introduction." Cybersecurity and Outer Space Essay Series, Centre for International Governance Innovation, January 29. www.cigionline.org/articles/securing-the-new-space-domain-an-introduction/.

Singel, Ryan. 2008. "Pakistan's Accidental YouTube Re-Routing Exposes Trust Flaw in Net." *Wired*, February 25. www.wired.com/2008/02/pakistans-accid/.

The White House. 2020. *National Space Policy of the United States of America*. Washington, DC: The White House. December 9. https://trumpwhitehouse.archives.gov/wp-content/uploads/2020/12/National-Space-Policy.pdf.

———. 2022. "Fact Sheet: Vice President Harris Advances National Security Norms in Space." Statements and releases, April 18. www.whitehouse.gov/briefing-room/statements-releases/2022/04/18/fact-sheet-vice-president-harris-advances-national-security-norms-in-space/.

United Nations. 2022. "General Assembly Adopts over 100 Texts of First, Sixth Committees Tackling Threats from Nuclear Weapons, International Security, Global Law, Transitional Justice." Press release, December 7. https://press.un.org/en/2022/ga12478.doc.htm?uuid=wJs1P74Xfhi3nZgl0332.

UNOOSA. 2017. *International Space Law: United Nations Instruments*. Vienna, Austria: United Nations Office. May. www.unoosa.org/res/oosadoc/data/documents/2017/stspace/stspace61rev_2_0_html/V1605998-ENGLISH.pdf.

———. 2022. *Annual Report 2021*. Vienna, Austria: United Nations Office. June. www.unoosa.org/documents/pdf/annualreport/UNOOSA_Annual_Report_2021.pdf.

Van Eeten, Michel J. G. and Milton Mueller. 2013. "Where is the Governance in Internet Governance?" *New Media & Society* 15 (5): 720–36.

West, Jessica. 2023. "The Open-Ended Working Group on Space Threats: Recap of the Second Meeting, September 2022." Waterloo, ON: Project Ploughshares. January. www.ploughshares.ca/reports/the-open-ended-working-group-on-space-threats-recap-of-the-second-meeting-september-2022.

Winner, Langdon. 1980. "Do Artifacts Have Politics?" *Daedalus* 109 (1): 121–36.

Wu, Timothy. 1997. "Cyberspace Sovereignty? — The Internet and the International System." *Harvard Journal of Law and Technology* 10 (3): 647–66.

Centre for International
Governance Innovation

67 Erb Street West
Waterloo, ON, Canada N2L 6C2
www.cigionline.org

@cigionline